RESEARCH
Influence and insight
through social media

November 2020

SASE BUYER'S GUIDE

The Next Frontier for IT: Multi-Cloud Companies Need a New Solution Combining SD-WAN and Security Functions

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

INTRODUCTION: SASE IS THE NEXT FRONTIER FOR THE NETWORK AND SECURITY

When executives talk about the corporate IT network, security usually dominates the discussion. However, it's hard to talk about security without considering networking. As a result, it's time to break down the network and security silos. For years, industry players have called for a convergence of strategies and solutions to more tightly bind networking and security. Now, that call is being answered with a fresh and promising approach.

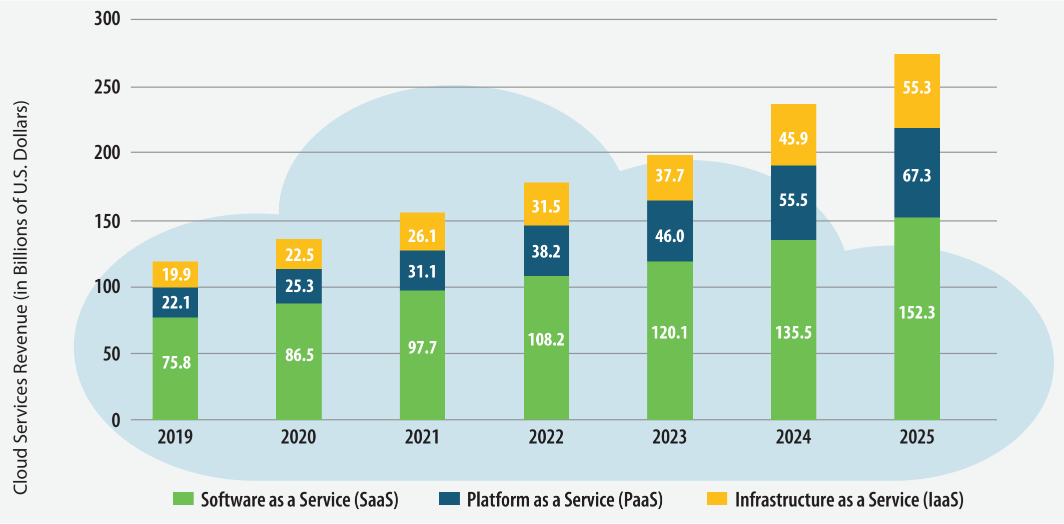
A great leap forward from idea to reality is uniting these two IT domains in a new category of solutions called secure access service edge or SASE (pronounced "sassy"). This guide will help IT executives understand what SASE is, why it serves as the new foundation for the future, and which considerations can help them make smarter investments in this emerging market.

SD-WANs, Security and the Cloud Must Evolve in Sync

The need for network and security convergence becomes sharply apparent as IT executives face the challenges of digital transformation on a global scale and at today's rapid pace of change. As digital transformation accelerates in enterprises, companies are adopting cloud services—often from multiple providers—to enable new projects and work-from-anywhere strategies. The ZK Research 2020 Global Cloud Forecast shows that cloud services will grow at an estimated 16% compound annual growth rate (CAGR) between 2019 and 2025 (Exhibit 1). That is ten times the estimated 1.5% growth of traditional on-premises applications, which underscores just how fast companies are shifting to the cloud.

The move to the cloud has profoundly impacted the network, particularly the wide-area network (WAN) and the edge, where distributed branch locations and remote workers continue to expand.

Exhibit 1: Cloud Continues Its Aggressive March to Dominance



ZK Research 2020 Global Cloud Forecast

The architecture used to build legacy networks (designed more than 30 years ago, when client/server and best-effort traffic was the norm) was intended to provide fast, reliable and secure access to data center applications. Consequently, almost all application traffic stayed "on-net" or flowed over the internal network, simply traveling directly from Point A (the data center) to Point B (the branch offices). The rapid shift of apps to the cloud means that the center of gravity has moved from the data center to locations out of the WAN and at the edge. The corresponding shift in traffic patterns to accommodate today's distributed environments has been drastic.

The once simple mission of the WAN has grown exponentially. Not long ago, the security perimeter and the network perimeter were the same thing. Now that employees are working from home and on mobile devices regularly, the WAN must reach beyond its legacy roots. The software-defined WAN (SD-WAN) solves most of those problems, but its capabilities must be extended in order to become a comprehensive solution that fulfills the modern enterprise's needs. SASE builds on the SD-WAN foundation and brings together both the network and security. With a range of features, SASE enables the network to securely extend resources to employees no matter where they are.

SECTION II: THE NEXT STEP—SD-WANS AND SECURITY COME TOGETHER

Let's take a look at the state of SD-WANs and how they can evolve to serve the modern enterprise's needs more effectively. One thing is certain: SD-WANs are great at the task they were designed to perform, which is evolving the transport of the WAN. In the cloud era, there's nothing better than an SD-WAN to connect to the various assets scattered throughout a company. If employees are in an office, at home or on the road, they have the ability to call up cloud data, connect to branch offices and communicate with colleagues seamlessly.

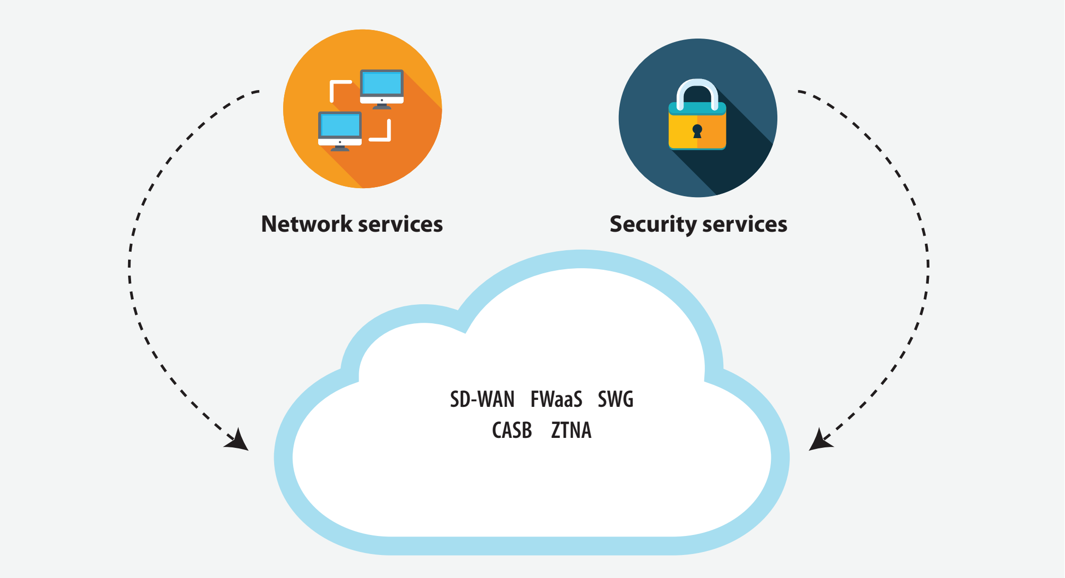
SD-WANs have certainly increased network reliability and have enabled a leap in application performance. Consequently, they are positioned to expand beyond their current footprint to address all WAN issues. However, as currently conceived, most SD-WANs leave out one critical ingredient that causes concern for everyone in an organization, from front-line workers up to the board room: security. If security is considered, it's usually an overlay slapped on top of the SD-WAN, running separately. With the digital experience, working from anywhere, mobility and the Internet of Things (IoT) throughout the network growing like weeds, this security arrangement is no longer effective. The attack surface has expanded while the capabilities of SD-WANs and security overlays to cope have not.

The world is ready for a change. The convergence of SD-WANs and robust security (Exhibit 2) in the form of SASE addresses the issues outlined earlier, creating a foundation for even more convergence and the next frontier.

SECTION III: INTRODUCING SASE

So, just what is SASE? In short, this new category of solutions combines WAN capabilities with network security functions. SASE solutions build on the SD-WAN foundation to bring together a

Exhibit 2: SASE Converges Network and Security Services



ZK Research, 2020

range of network and security capabilities into a distinct cloud-based service from a single provider. The SASE solution should include five critical components:

SD-WAN: The SD-WAN has moved the network away from being tied to specific hardware, which lowers enterprises' costs while providing them access to higher performing WANs that can use available internet access.

Firewall as a service (FWaaS): The FWaaS enables customers to move the functions of a firewall from on premises to the cloud. It should also be able to function on-premises when needed.

Secure web gateway (SWG): The SWG stops unauthorized web traffic from breaching an organization.

Cloud access security broker (CASB): The CASB works between cloud service users and cloud applications to observe traffic and ensure security policies are enforced.

Zero trust network access (ZTNA): This approach trusts no one until they present verification to gain access to the network with the default being an access of "least privilege."

The unification of these five separate solutions into a single cloud platform reduces IT complexity and provides the IT organization with ease of management. The result is a synergy across both IT domains; under the SASE model, network and security have officially come together. The management capabilities of SD-WANs and software-defined networks are centralized via a unified policy orchestrator with one portal. This is where all of SASE's critical components interoperate, providing end-to-end visibility and control. Under this single operating system, SASE has the potential to become a much bigger cloud platform—expanding beyond the five components that define it today.

Let's take a close look at the earmarks of SASE:

SASE is cloud based and delivered as a service. This helps companies shift easily from the hardware-focused world of on-premises, data center–focused networks to the software-based SASE environment. At the same time, multi-tenancy translates to reduced costs and the ability to support the burgeoning remote, distributed and mobile workforce.

SASE has a global footprint that is ideal for companies that are geographically dispersed. Consequently, companies doing business across multiple regions or countries can connect with low latency across worldwide points of presence.

SASE focuses on user identities and individual devices rather than the data center. Access to identity analytics and user activity tracking capabilities is baked in.

SASE services emphasize flexibility and security at the edge, where branch locations, cloud applications, and mobile and IoT devices connect.

SASE is ideal for highly distributed organizations and aligns well with companies undergoing a cloud migration as well as the massive trend toward remote and mobile workers.

SECTION IV: WHAT TO LOOK FOR IN A SOLUTION PROVIDER

Finding a solution provider that can converge the wide swath of components outlined in the previous section can be a challenge. Businesses need a company with a broad set of skills, extensive partnerships and delivery expertise. For SASE to be effective, businesses need a provider that takes a holistic approach to the network, security, the cloud and beyond. Here are some key considerations:

Unified security from industry leaders: The threat landscape has expanded amid today's cloud and work-from-anywhere trends. That means companies must protect themselves and their data using a variety of best-of-breed solutions from leaders in the security industry. However, SASE technology stacks are not always built this way. Rather than consolidating leading technologies from other companies, some SASE providers build their own security products from the ground up because it can be a challenge to combine multiple security products from a wide variety of vendors into one service. However, consolidation is better for the customer because it provides them the benefits of proven protections via a one-provider service experience.

When it comes to security, businesses should consider looking beyond SASE. SASE's short list of security requirements is just one piece of the equation for the cloud and work-from-anywhere trends. Businesses that limit their focus to SASE will likely miss many other critical security vectors. For example, is a provider planning to extend SASE to cloud security, security operations center (SOC) services and analytics? Are any incident and response plans on the vendor's radar? It's important to remember that they must cover all IT domains, including network, endpoint and cloud.

Cloud options: With today's cloud-centric approach to remote work and digital business, a provider should offer SASE as a cloud-delivered and cloud-managed solution. Every SASE component should be developed to run on globally distributed and highly available infrastructure administered from a centralized cloud-based user interface. A retrofitted, updated, rebadged or recoded version of previous network and security offerings won't cut it. A globally distributed network is critical so that organizations can access resources no matter where they are on the planet. As noted earlier, providers also need to include a hybrid firewall with SASE that works in the cloud and can also function on premises for more extensive operations.

The terms "cloud delivered" and "cloud managed" might seem the same but are quite different, and each serves a purpose. For SASE to be cloud delivered, it must be engineered from the ground up to run all functions in the cloud. The only piece of on-premises infrastructure is the lightweight SD-WAN device, which connects users to the SASE. Everything else is developed and deployed in the cloud. This is ideal for work-from-home (WFH) scenarios and smaller offices with just a few people in them.

With cloud-managed solutions, the infrastructure remains on premises but is managed from the cloud. In this case, the network and security services run on physical or virtual appliances in the branch office. This is better for large locations with dozens or hundreds of people, as the amount of traffic generated going to and from the cloud for inspection purposes could be more than the actual data traffic.

Performance: With SASE services so dependent on cloud infrastructure, it is only logical that network stability is crucial for a successful deployment. Delivering a reliable, low-latency SASE service is difficult when the provider either has no control over the last mile of IP transit or has no visibility beyond its core network. The inherent ability of SD-WANs to leverage multiple broadband links and forward error correction can help mitigate some of these issues. But most enterprises will want a SASE provider with a service-level agreement (SLA) using high-availability service options that connect via multiple last-mile service providers to redundant security points of presence and power supplies. Without a strong SLA, the SASE service runs the risk of not working and clients run the risk of having no remedies or penalties should the service levels not be achieved.

Service flexibility: Unlike the SD-WAN connectivity between office branches that some enterprise IT departments deploy themselves, the overall complexity of SASE precludes a "do it yourself" deployment for most companies. By sourcing a SASE solution from a managed services provider, companies can have a turnkey deployment with monitoring and management included. A SASE solution should be available with both managed and co-managed services so that a company can choose the level of support it needs based on its specific circumstances.

Evolving and innovative solutions: SASE is an emerging framework and a great starting place for network/security convergence. In a short time, it has made incredible progress. But much like SD-WAN, SASE has room to evolve and grow. So, businesses should look for a provider with a roadmap that moves SASE toward encompassing additional security needs as well as technological innovations. For example, can the provider articulate its vision for combining artificial intelligence (AI) and SASE to create AI for IT operations (AIOps), which provides the intelligence needed for network automation and autonomous networking? The items on the roadmap should have some details behind them; they shouldn't just be words on a whiteboard or a presentation slide.

Above all, businesses should look for a provider known for service excellence. Rolling out a SASE across the enterprise is, to an extent, an exercise in trust. Businesses need to trust that the vendor they choose will be with them every step of the way. Therefore, it's important to vet vendors against the points outlined in this section, check their net promoter scores and get an iron-clad support commitment.

The Next Frontier

SD-WANs solve software-as-a-service (SaaS) challenges, and now SASE is solving cloud and WFH security challenges. Soon, SASE will be making strides toward the autonomous future.

SECTION V: MASERGY DELIVERS BEST-IN-CLASS SASE

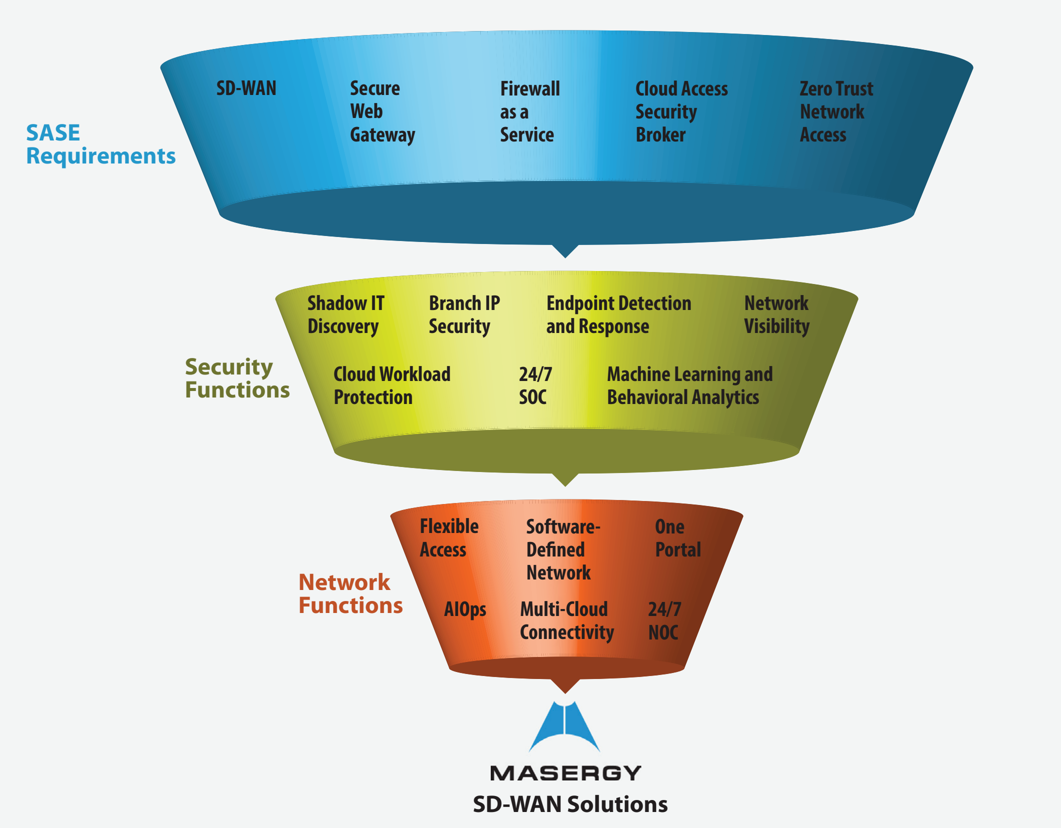
With more than 1,600 enterprise clients and 20 years as a pioneer in software-defined networking, Masergy is well positioned to deliver best-in-class SASE solutions.

Masergy addresses the five major aspects of SASE, as defined by ZK Research (Exhibit 3):

Security-first SD-WANs: Masergy's solution includes Fortinet technology that ensures a security-first approach to SD-WANs, including a next-generation firewall and SWG. Fortinet excels at security and SD-WAN networking, as evidenced by its placement as a Gartner Magic Quadrant Leader for WAN edge infrastructure and next-generation firewall.

The Masergy approach to a security-first SD-WAN means enterprises get the full spectrum of security they need to protect their data no matter where it resides—in a data center, on premises,

Exhibit 3: **Masergy Offers a Complete SASE Solution**



Masergy and ZK Research, 2020

in the cloud or otherwise. Masergy's solution also includes a comprehensive set of security tools, analytics and SOC monitoring that comes with unified threat management capabilities, Masergy's SOC and three tiers of security services—coupled with more than a decade of leadership in managed security services. In addition, Masergy's SD-WAN offerings bring together a unique array of security solutions that include embedded shadow IT discovery and identity-based WAN analytics.

Cloud firewall: Masergy's flexibility with firewalls means an enterprise can place them either in the cloud or on premises. Masergy also built Fortinet's next-generation firewalls into the SD-WAN, so putting security at the edge is simple. Cloud-based firewalls are agile and perfectly suited to smaller offices. Fortinet appliances are ideal for large offices that need high performance and lower TCO. Neither choice is better, per se, and Masergy leaves the choice up to the customer and will support it either way.

Secure web gateway: Masergy integrated Fortinet's SWG into the SD-WAN. With cloud-based application control and content filters, enterprises gain granular visibility both per app and per user, along with identity-based WAN analytics.

Cloud access security broker: Masergy enables proactive management with a CASB from Bitglass that deploys and produces value quickly. The CASB gives enterprises the ability to handle security risk and accelerate their cloud strategies confidently.

Masergy's solution is fully managed and benefits from the company's SOC alerting and incident response 24/7, so the IT team can focus on pressing matters rather than day-to-day security headaches. In addition, cloud workload protection powered by Trend Micro secures migrations to infrastructure as a service (IaaS) and platform as a service (PaaS) and mitigates public cloud risks. And for enterprises that need visibility into their Office 365 security posture, Masergy offers security monitoring into that important set of productivity tools.

Zero trust network access: Masergy's SD-WAN security includes highly rated endpoint detection and response (EDR). Plus, it provides per-user statistics across all applications, including user activity information and tracking.

Masergy's managed detection and response approach puts the company's certified security analysts to work for enterprises that not only are monitoring security but also are ready to craft a prioritized threat response plan and act on it. Masergy continues to build out ZTNA capabilities with a near-term roadmap that includes single sign-on (SSO); authentication and authorization based on user, device and location; and varying levels of access.

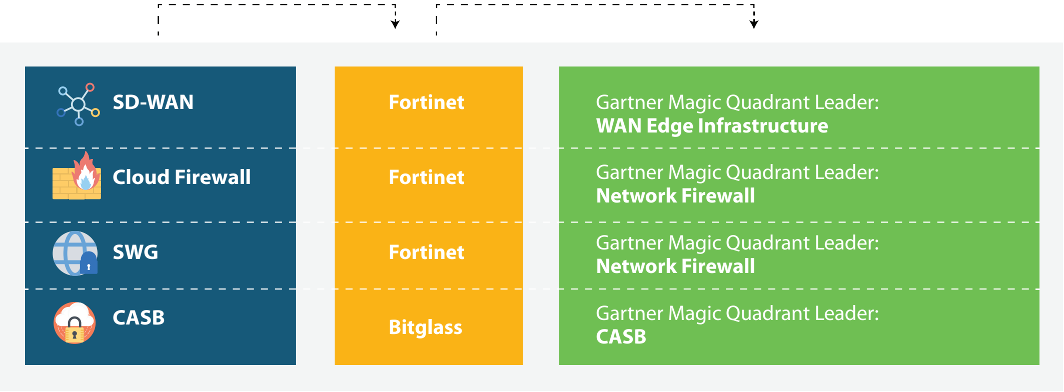
Best-of-Breed Solutions and Best-in-Class Architecture

In ZK Research's opinion, Masergy's offering is unique in a couple of ways. First, it brings best-of-breed providers together into a single, software-defined architecture to deliver a simple cloud-based service that minimizes daisy chains. Second, Masergy embeds the technologies into the network fabric, and the service is managed online with network and security analytics in a single portal. The SASE elements feature solutions from world-class providers (Exhibit 4).

Industry-Leading Network Edge Performance

Masergy's SASE is a significant innovation for multi-cloud enterprises that require unrivaled application performance. At the core of the SASE framework lies Masergy's SD-WAN. The company's global network was software defined before software defined was cool. That's how it can reliably deliver reduced capex and improved agility and performance as well as help customers avoid technology obsolescence. Masergy is an industry pioneer, and for two decades, it has been serving

Exhibit 4: Masergy Ties Together Best-of-Breed Technologies into One Solution from One Provider



SD-WAN	Fortinet	Gartner Magic Quadrant Leader: **WAN Edge Infrastructure**
Cloud Firewall	Fortinet	Gartner Magic Quadrant Leader: **Network Firewall**
SWG	Fortinet	Gartner Magic Quadrant Leader: **Network Firewall**
CASB	Bitglass	Gartner Magic Quadrant Leader: **CASB**

ZK Research, 2020

global enterprises of all sizes with a secure cloud and network platform that delivers less than 1 millisecond of jitter.

SECTION VI: CONCLUSION AND RECOMMENDATIONS

Digital transformation is disrupting the business landscape faster than ever, which is placing an emphasis on the optimization of IT resources to increase the speed and delivery of new services. To accommodate these changes and improve the agility of applications and remote workforces, organizations are adopting new technologies such as containers, cloud computing and mobility.

However, during this time, the network—particularly the WAN and network security architectures—has remained largely unchanged and consequently is holding organizations back from becoming digital leaders. Companies that can't make this shift risk falling behind and becoming irrelevant—quickly. Software-defined networking has had a major impact on data centers, and its power to transform the WAN has given rise to more modernized and agile alternatives (e.g., SD-WANs) to the rigid legacy networks that have been in place for more than three decades. SASE takes SD-WANs to the next level with the integration of security and the shift to cloud-native platforms and cloud-management solutions. Therefore, implementing a SASE solution must be a top initiative for IT and business leaders.

To help company leaders make this transition to SASE, ZK Research offers the following recommendations:

Consider the network to be the most strategic IT asset in the organization. All digital technologies are network centric, from the cloud to IoT to artificial intelligence. If the network doesn't work, neither does the business. For most companies, this means the network *is* the business. Therefore, C-level executives must understand this and invest in a next-generation network to power their business into the digital age.

Embrace the cloud for networking. Almost every part of the IT stack has shifted to the cloud model. One of the few holdouts has been the network, particularly the enterprise WAN. SASE enables the delivery of robust cloud and network services anywhere an organization does business without the headache and challenges of on-premises infrastructure. But it's important to understand that cloud management of on-premises infrastructure can be just as effective as cloud delivered. The key is to leverage the cloud where it makes sense to do so.

Consider a managed service approach. Although SASE simplifies network operations, getting to SASE can be a complex set of tasks. It involves deploying an SD-WAN first and then considering all the security implications, including those of work-from-anywhere employees. A viable option for most companies is to leverage the expertise of a managed service provider to manage or co-manage the network with the organization and assist with threat detection and response. This enables the shift to SASE without the associated risk.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314